EXHIBIT 1

Legal Department Procedure No. 3.1

EFFECTIVE DATE: ***October 10, 2023***

PROCEDURE TITLE:

Records Management Implementation Procedure

To be reviewed every three years by:
Executive Vice President and Chief Legal Officer

REVIEW BY: ***November 1, 2026***

PROCEDURE

This Procedure is intended to implement Legal Department Policy No. 3 - Records Management. Specifically, this Procedure establishes a consistent process for the required retention and destruction of business records ("Records"), in order to maintain Records for only as long as they benefit the company and as necessary to comply with all legal and regulatory requirements. This Procedure describes the requirements for systematic control of Records from the time of creation until ultimate destruction, including the collection, recording, storing and eventual discarding of information.

Roles and Responsibilities

Record Ownership and Destruction: Trinity Health is the owner of all Trinity Health Records, whether hard copy or electronic. Trinity Health has the right to review for any purpose and assess the continued need for any and all Records, at any time.

User: Users of information at Trinity Health are permitted to access, utilize, and create Records in order to perform duties related to their job. Each User is the custodian of information in the Records, and is responsible for ensuring that all Records in their possession or under their control are maintained in compliance with the Trinity Health System-wide Records Management Schedule. Users are responsible for understanding all Record types and for categorizing the User's Records according to the Records Management Schedule in collaboration with the User's Department Head.

Users leaving Trinity Health may not take Records or copies of Records with them, unless specifically authorized by appropriate senior management. Permission generally is not granted if the records contain intellectual property or confidential business information. Permission is necessary even if the Records do not contain intellectual property or confidential information and the User only wants them as writing samples or mementos.

Information Systems: Trinity Information Services (TIS) will maintain backup and retrieval capabilities for all electronically stored data on Trinity Health owned and managed devices that store electronic data, including laptops/desktops, servers, network drives and mobile devices. TIS will be responsible for backup and recovery of all Functional Record Types on these devices. Department Heads will require Department Users to connect to the network on a regular basis. TIS will be responsible for destroying backup files of electronic storage of data in accordance with backup retention periods established by the TIS department in accordance with the Functional Records Management Schedule. TIS will not be responsible for routine destruction of data or information on shared drives, laptops or local hard drives. Department Heads and Users are responsible for directing TIS regarding required destruction.

Applications: TIS will be responsible to backup all TIS supported applications as needed for disaster recovery and business continuity.

User and Shared Network Drives: All User (personal) and shared network drives will have an individual User identified as the owner of the drive. TIS will back-up all information on User and shared network drives. The User, as directed by the Department Head, is responsible for identifying Records and purging them on User and shared network drives after the retention period has expired as specified in the Functional Records Management Schedule.

Mobile Devices: The User, as directed by the Department Head, is responsible for identifying Records and purging them on mobile devices after the retention period has expired as specified in the Functional Records Management Schedule.

Electronic Mail: Electronic mail messages should be deleted by the User once they have served their purpose. Electronic mail messages on mail servers are automatically deleted after six (6) months. Email messages that are needed for business purposes must be transferred by the User (generally contemporaneously with receipt of the message) to an appropriate filing system (for example, printed and then filed, or saved as an electronic file). Users are responsible to store emails and attachments that are Records in a separate system (User's network drive, shared drive, paper copy, etc.). Calendar Records are automatically deleted after one year.

Voice Mail: Voice mail messages must be deleted once they have served their purpose. The recipient is responsible for retention in an appropriate filing system and disposal of any Record that he/she determines is needed for business purposes.

Back-ups: Back-up copies may be accessed only for restoration and may not be accessed by Users or for routine business operations.

Records Management Responsibilities of Department Heads and Departments:

Department Head: Department Heads are responsible for ensuring the retention and disposal of Records that were created by Users in the department and Records accessed and retained (including copies of originals) by Users in the department. Each Department Head is responsible for providing direction and oversight of the retention and disposal of Records stored on computer systems maintained by Trinity Information Systems (TIS) and cloud service providers whose services are approved by TIS and contracted by the Department as business owner, unless responsibility has been otherwise expressly assigned to another Trinity Health function. Each

Department Head also is responsible for providing direction and oversight of the retention and disposal of paper copies and physical Records stored on-site or off-site. Department Heads will require Department Users to connect to the network on a regular basis for backup purposes.

A Department Head is responsible to develop Records Management processes for the department, develop the classification scheme used for the department for paper files, and for electronic files on the shared drive, and appoint a Records Management Coordinator for the Department in accordance with this Procedure and the Records Management Policy and Functional Records Management Schedule.

The Department Head is responsible to name and exercise oversight of the department's Records Management Coordinator. The Department Head may delegate additional Records Management duties as appropriate; review new procedures or improvements suggested by the Records Management Coordinator; resolve issues raised by the Records Management Coordinator or by others in the department; monitor compliance with department Records Management Procedures; and oversee compliance with Legal Holds affecting the department.

Department Records Management Coordinator: The Department Records Management Coordinator must have the time, authority and responsibility to manage and coordinate the Records Management Program within the department. The Records Management Coordinator is responsible for conducting an annual compliance review and verifying that all department Records have been reviewed and disposition made by the custodian of those Records. The Records Management Coordinator also is responsible for ensuring that all Records used by the department are being stored in an efficient and organized manner and are available when needed; ensuring that appropriate procedures for offsite storage are followed; and interpreting and answering questions about the Records Management Policy and Procedure for their department. The Records Management Coordinator assures that Records are reviewed and reassigned when a User leaves the department.

Records Management Committee (RMC) (Optional): The Ministry may establish a RMC. It is suggested that the RMC consist of representatives of the following departments: Finance, Health Information Management, Human Resources, Information Security, Information Services, Legal, Insurance and Risk Management Services and Organizational Integrity and Audit Services. The RMC's responsibilities may include: Develop and communicate management expectations for Records Management; develop the Records Management Processes and Policies within all functions; serve as a technical resource for Records Management questions; spot review for compliance with Trinity Health Records Management Policy and Procedures; develop and maintain a network of department records management coordinators; define company records.

Record Lifecycle Management

Identification/Labeling of Records: Records must be kept in an efficient and organized manner in accordance with current Enterprise Information Security procedures. All files (including computer files/removable media) must be labeled reflecting the contents of the file. Each Record must include the ability to determine the date of creation, and the person or function that created or is responsible for the Record. Most Records require the date and identification of the author.

However, for a few types of records, the date and identity are not necessary. These include business cards, blank letterhead and postings/sites that display messages.

Annual Review: At a minimum, annual reviews should be conducted of Policy and Procedure compliance for a representative sample of Users. Ministry management determines who conducts the audit. The group conducting the review should have the specialized expertise to review electronic Records, or should obtain the assistance of a qualified expert. The review of electronic Records may, but need not, coincide with a review of paper records.

Record Disposal: When records reach the end of their retention period, the method of disposal must effectively eliminate the Record so that the information/data is destroyed. When paper documents containing confidential information or PHI are no longer needed, they are disposed in a manner that protects their confidentiality (shredding, pulping, or burning). Confidential information awaiting destruction should be protected in locked containers or in a private location in a locked room or suite. Records on hard disks may be removed by destroying the actual hard disk, or data wiping the entire hard disk. Records stored on removable media must be destroyed so the information is not retrievable. Options include physical destruction, utilizing software to overwrite data through data overwriting, or degaussing. Destruction obligations also apply to Records stored on home computers if used for Trinity Health Records. It is recommended that Users not store Trinity Health Records on the hard drive of a home computer. It is preferable to use a network resource (such as a file server) for storage so that proper electronic Record back up and disposal is performed. Department Heads and Department Records Management Coordinators are responsible for overseeing compliance of Users who use home computers in connection with work functions.

Record Lifecycle Management – Special Issues

Orphaned Records: A Trinity Health User/department may find or inherit Orphaned Records. Orphaned Records may originate from either an external (e.g. merger, acquisition) or internal (e.g. closed hospital, Novell server files, job assignment change) source. The User/department with custody of Orphaned Records will (1) employ reasonable efforts to identify a department to be the "owner;" and (2) if those efforts are successful, assign the records to that "department owner." The owner department will be responsible for compliance with retention schedules for those Records. If reasonable efforts are not successful in identifying another department as the "department owner" then the department with custody of the Records is responsible for compliance with retention schedules for those Records.

Transferred or Separated User: When a User is transferred or leaves Trinity Health, all Records held by that User are to be assigned to another User in the same department. TIS is responsible for updating/terminating access and for maintaining and storing emails, voice mails and other Records for the record retention time periods required by the Records Management Schedule. A transferring User's ability to access to these Records must be removed, unless his/her new Trinity Health job requires continued access and the Department Heads agree on continued access.

Trinity Health Records in Transit: Trinity Health Records in the custody of Users and in transit must be handled securely as required by Enterprise Information Security and, if applicable, Privacy procedures. Paper and physical Records must be stored in locked locations and not left unattended.

Electronic Records must be transmitted in a secure manner. If removable media is used for transmitting Trinity Health Records, the media must have full-disk encryption enabled.

Trinity Health Records in Users' Homes: Trinity Health Records in the custody of Users working out of their homes have the same retention obligations and schedule as Records on Trinity Health premises.

Records Subject to Legal Hold: All Records will be disposed of at the end of their retention period unless the Records are subject to a written Legal Hold order by the office of the General Counsel or designee. If a Legal Hold is in effect, Records subject to the hold must not be destroyed until termination of the Legal Hold in accordance with the Legal Hold Policy and Procedure.

Records Held By Third Parties: Department Heads and Users are responsible for ensuring compliance with applicable retention schedules when a third party (e.g., Iron Mountain, Corrigan, cloud services provider) has custody of a Trinity Health Record.

Records Containing Payment Card Industry (PCI) Data: PCI data should not be stored. When storage of patient payment information is necessary, the only permitted elements are:

- Cardholder Name;
- Expiration date;
- Primary account number with only the first six (6) OR the last four (4) characters displayed; and/or
- Service code.

Loss of Ability to Read or Access Records: If a storage medium cannot handle the full retention schedule of a Record (i.e., outdated technology) for the required record retention time period, provisions must be made to transfer the Record before it becomes unusable. If the information that is not stored includes the author's signature or initials, there must be some other way to identify the author of each Record.

Record Formats and Copies

There is one official retention copy of each Record. It may be the original or a copy. Searching or sorting a file (e.g., rearranging data items in excel by specified criteria) does not in itself create a new Record. However, distributing the newly sorted version in effect creates a new version of the Record (for example, you send copies to people) and the Record must be preserved.

Copies of a Record, including back-up copies and drafts, are permitted. However, they may not be kept longer than the retention schedule for that type of Record. Users are permitted to create a back-up copy of electronic Records to safeguard against accidental loss. Back-up copies should only be created when there is a sufficient need.

The "starting date" for Records retention of a final document is the date when the final document was created or fully executed if the document is a signed document. This date is normally written

in the document. Many computer systems will also have an electronic date indicating the date the document was last saved. The directory date is not the controlling date for Records retention, but may be used if it is generally consistent with the date written in the document.

Sticky notes and similar comments used in business operations must be attached to and filed with the applicable Record. The sticky note must be labeled with the date and author of the note. The sticky note has the same retention schedule as the Record.

Temporary communications do not constitute Records. Temporary communications are intended to be acted upon, or otherwise serve a purpose, in a short period of time, and do not fall into any of the categories of documents with specific retention times, in the Trinity Health Records Management Schedule. Once the temporary communication has been acted upon and served its purpose, there is no ongoing business need or legal requirement to retain the communication. The destruction process for temporary communications must include spot checks to ensure accurate entry of data, scans, etc. Examples include most telephone messages conveying time, location or contact information, inter-office transmittal memos, replies that require no new decisions or administrative action, meeting notices, requests for a return telephone call, most draft documents, electronic "scratch pads," and "to do" lists, handwritten documents used to input data into electronic Records and personal notes. Most drafts have served their purpose when the next draft (or the final document, if there is no "next draft") has been prepared.

Records Management on Removable Media

Records Management requirements for removable media apply not only to "Trinity Health" media, but also to Users' personal media if personal media contains Trinity Health Records.

Encryption: Electronic information stored on personal devices or removable media must have full-disk encryption enabled as required by Enterprise Information Security procedures.

Labeled Removable Media: Proper subject labels are required for removable media. Labels should include the date of creation, and be visible on the outside of the removable media. In cases where a physical, visible label is not possible (as with hard disks), folders or files holding the Record must be labeled.

Destruction: When a Record reaches the end of its retention time, the method of disposal must effectively eliminate the Record. That can be difficult if the removable media also contains other documents that have not expired. Accordingly, Records with different retention periods should not be stored on the same removable media. Records with different expiration dates stored on a single removable media, must be reviewed annually for expired retention periods.

SCOPE/APPLICABILITY

Health Ministries and Subsidiaries (not first tier). This Procedure is intended to apply to all Colleagues of Trinity Health, its Health Ministries or Subsidiaries. Each Trinity Health Ministry and Subsidiary is required to implement the Records Management Program established by Legal Policy No. 3 - Records Management and this Procedure, and to comply with the Trinity Health Records Management Program.

Transitioning New Subsidiaries to Trinity Health's Program: Typically, a new Ministry or Subsidiary will need time to transition to Trinity Health's Records Management Program. The transition will be included in the onboarding of the new Ministry or Subsidiary and coordinated with Trinity Health Legal and Insurance and Risk Management Services Departments. An appropriate schedule will be established for demonstrating compliance. Coordination should begin as early as practical. This coordination may include appropriately limited interaction before Trinity Health acquires ownership.

DEFINITIONS

Department means a work unit.

Department Head means the individual who is lead for a Department of a Ministry.

Department Records Management Coordinator means the employee who has been appointed for each Ministry or Subsidiary department. The Records Management Coordinator must have the time, authority and responsibility to manage and coordinate the Department's Records Management Program.

Executive Leadership Team ("ELT") means the group that is composed of the highest level of management at Trinity Health.

Ministry (sometimes referred to as Health Ministry) means a first tier (direct) subsidiary, affiliate, or operating division of Trinity Health that maintains a governing body that has day-to-day management oversight of a designated portion of Trinity Health System operations. A Ministry may be based on a geographic market or dedication to a service line or business. Ministries include Mission Health Ministries, National Health Ministries, and Regional Health Ministries.

Local Hard Drives in a personal computer are often called a "disk drive," "hard drive," or "hard disk drive," is the local unit, typically internal, that stores and provides relatively quick access to large amounts of data.

Policy means a statement of high-level direction on matters of importance to Trinity Health, its Ministries and Subsidiaries or a statement that further interprets Trinity Health's, its Ministries' and Subsidiaries' governing documents. Policies may be either stand alone, systemwide or mirror policies designated by the approving body.

Procedure means a document designed to implement a policy or a description of specific required actions or processes.

Proprietary Information means information that is confidential business information including patient, employee/colleague and financial information.

Record(s) means any format or medium in which information relating to the business of Trinity Health, its Health Ministries and Subsidiaries is stored, including without limitation, paper documents, electronic mail, instant messages, electronic calendar information, electronic database entries, and voicemail messages. Records do not include temporary communications such as voice messages requesting a return call or advising of a lunch location and not reflecting business

operations or the conduct of business. As further illustration, Records include, but are not limited to:

- Computer-generated Records;
- Documents created using word processing programs, spreadsheet programs, or other software, and stored electronically;
- Voice mail messages;
- Computerized calendaring and time management systems;
- Electronic mail messages;
- Intranet/Internet transmissions;
- Records transferred (by scanning, fax, data input, etc.) from paper or other "hard copy" into a computer;
- Facsimile (fax) documents received on a computer and stored electronically;
- Information/data on removable media (floppy disks, hard disks, optical disks, etc.);
- Records on magnetic tape; and
- Audiotapes and videotapes, including dictation cassettes.

Records Management Committee (RMC) means the optional multi-disciplinary committee established to provide oversight relating to a Ministry's Records Management Processes.

Records Management Schedule means the Trinity Health Records classification system by which Record retention periods are determined for classes of Records based on the fiscal, operational, historic and legal value of the Record class. The Trinity Health Legal Department shall maintain a schedule setting forth the legally required retention periods for classes of Trinity Health and Ministry Records.

Removable Media refers to computer storage devices that are not fixed inside a computer. These devices can be usually transferred easily from computer to computer and typically use external interfaces such as USB and FireWire. Examples: Compact Flash, CDs, External Hard Drives, Floppy Disks, Multimedia Cards, SD Cards, USB Flash Drives (Thumb Drives).

Shared and Personal Drive(s) means data storage units that store information on a hard drive or common server with limited access for User(s). Shared drives allow multiple Users access to data so that they can share information.

Subsidiary means a legal entity in which a Trinity Health Ministry is the sole corporate member or sole shareholder.

User means an individual who is the custodian and/or owner of Records.

RESPONSIBLE DEPARTMENT

Further guidance concerning this Procedure may be obtained from the Legal Department.

RELATED PROCEDURES AND OTHER MATERIALS

- Functional Records Management Schedule

- Legal Department Policy No. 3 - Records Management
- Legal Department Policy No. 4 - Legal Hold
- Privacy and Finance procedures regarding storage and destruction
- Enterprise Information Security Procedures regarding security and storage, e.g. TIS 4.0 Asset Management (in process)
- Trinity Health "Guidelines for Procedure Development"

APPROVALS

Initial Approval: August 1, 2007

Subsequent Review/Revision(s): February 20, 2019, October 10, 2023